



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR  | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|-----------------------|---------------------|------------------|
| 10/576,876      | 01/10/2007  | Howard William Winter | 011765-0350771      | 9924             |

909 7590 05/05/2009  
PILLSBURY WINTHROP SHAW PITTMAN, LLP  
P.O. BOX 10500  
MCLEAN, VA 22102

|          |
|----------|
| EXAMINER |
|----------|

VAUGHAN, MICHAEL R

|          |              |
|----------|--------------|
| ART UNIT | PAPER NUMBER |
|----------|--------------|

2431

|           |               |
|-----------|---------------|
| MAIL DATE | DELIVERY MODE |
|-----------|---------------|

05/05/2009

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

|                              |                                       |   |  |
|------------------------------|---------------------------------------|---|--|
| <b>Office Action Summary</b> | <b>Application No.</b><br>10/576,876  | <b>Applicant(s)</b><br>WINTER, HOWARD WILLIAM |  |
|                              | <b>Examiner</b><br>MICHAEL R. VAUGHAN | <b>Art Unit</b><br>2431                       |  |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 09 March 2009.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-23 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-23 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)          | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____  | 6) <input type="checkbox"/> Other: _____                          |

### **DETAILED ACTION**

The instant application having Application No. 10/576876 is presented for examination by the examiner. Claims 2-13 and 15-23 have been amended. Claims 1-23 are pending.

### ***Response to Amendment***

#### ***Claim Objections***

The current amendments overcome the previous claim objections.

#### ***Claim Rejections - 35 USC § 112***

The current amendments overcome the previous 112 rejections. Examiner is also withdrawing the 112 1st rejection.

### ***Response to Arguments***

Applicant's arguments filed 3/09/09 have been fully considered but they are not persuasive. Applicant has alleged that prior art, SCAMPI, fails to teach replicating said data on board a network analyzer card and producing two editions of data.

In response to the allegation that SCAMPI does not perform the copying on a network analyzer card, Examiner find support for this in pages 54-55. The SCAMPI protocol which includes the copying of data is performed by the SCAMPI adapter which

Art Unit: 2431

includes the COMBO6 motherboard and physically connected interface card. SCAMPI teaches the monitoring of data is executed in either software or hardware (last sentence page 6). It should be noted that all software processing is ultimately performed in hardware. One type of hardware SCAMPI explicitly teaches is monitoring hardware such as network processors. It appears the SCAMPI adapter is one example of this type of monitoring hardware. The functionality of the monitoring is broken down into software functions. However as mentioned, software is still executed by hardware. One type of monitor taught by SCAMPI is the MAPI. MAPI is taught to be co-located with the SCAMPI monitoring device, see first paragraph of section 2.4 on page 10. One function being performed by the MAPI is the creation of a new sub-flow containing only the packets of interest. This is equivalent to the claim's replicating data on board a network analyzer card. SCAMPI teaches that monitoring can be done in hardware **or** software. It appears to the Examiner the SCAMPI protocol uses their on developed hardware device (SCAMPI adapter) to directly interact with the data stream. In other words data stream processing is being performed by the device even in the case where software functions are being called. Again, SCAMPI explicitly teaches the monitoring can be performed by dedicated hard processors. Figure 2.1 shows a logical picture of what is happening in a modular diagram. However, there is no way to physically separate hardware from the software running on it. If SCAMPI teaches the monitoring jobs are done in hardware by a network processor, the SCAMPI adapter is capable of achieving this functionality. The middleware as taught by SCAMPI is not a separate piece of hardware from the adapter. The middleware is just more software functions.

The second point of disagreement concerns the way data is replicated. First of all, the term data is interpreted as a plurality of packets. The claim recites receiving data. Examiner interprets this receiving a packet stream. The notion of what constitutes editions is apparently different for the Applicant and Examiner. Google defines an edition to be:

“An edition is the total number of copies of a work printed at one time.”

In other words, an edition is all of the copies from a **single** work. Two editions would somehow be different from each other. Two editions are not equivalent to two copies. One edition can have many copies, but they are just that, exact copies. For example, if someone had two editions of the same book, they would somehow be different from each other. One would have two editions not just two copies. Examiner interprets the claim to mean copying the data packets of a data stream to produce at least one copy of each packet. The first data packet is copied producing an edition of that data packet and it is placed into its own buffer. The second data packet is copied producing an edition of the second data packet, and placed into its own buffer. The data packets are different, and therefore their copies( and editions) are different from each other. For every data packet copied you get a new edition and it gets placed into a buffer. Therefore, SCAMPI teaches this functionality as "all required packets are copied to the appropriate buffers", page 18. Applicant is interpreting the claim to mean each received packet is copied at least twice. However, there are other ways to broadly interpret the claim language.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 1-20 are rejected under 35 U.S.C. 102(a) as being anticipated by the SCAMPI Prototype Implementation Report D2.2 published on Nov. 16<sup>th</sup>, 2003, hereinafter D22.

As per claim 1, D22 teaches receiving data from a network link (pgs. 10 and 17); replicating said data on board a network analyzer card (pg. 55) to produce at least two editions of the received data (pgs. 18-19 and Fig. 2.6); and writing said editions of the received data to an area of memory in a host that is directly accessible by a host application (pgs. 19 and 25, particularly section 2.7.4).

As per claim 2, D22 teaches processing said editions of data stored in the said area of memory accessible by a host application, the processing comprising executing a different set of rules relating to intrusion detection on each edition (pg. 57).

As per claim 3, D22 teaches the data is replicated using hardware (pgs. 6 and 54).

As per claim 4, D22 teaches the editions of the received data are provided as independent data streams [unique packet buffers] (pg. 18).

As per claim 5, D22 teaches each of the at least two editions of said received data is buffered independently [has own buffer] (pg. 18).

As per claim 6, D22 teaches each of the independent data streams is filtered according to desired criteria (pg. 18, by classifiers and functions).

As per claim 7, D22 teaches different filtering rules are applied to each of the editions of the received data [each rule flow is created] (pg. 58).

As per claim 8, D22 teaches writing the editions of the received data to an area of kernel memory [kernel modules] of the host memory; (pg. 31 and 44) and providing to the host application an offset to enable location of the data by the host application in the kernel space of the memory (pg. 19, pointers).

As per claim 9, D22 teaches when data is written to the kernel space of the host memory a list of offsets with respect to a base address within kernel space is generated, the list of offsets serving to enable location of data packets within the kernel space with respect to the base address (pg. 19, pointer sets).

As per claim 10, D22 teaches providing to an application for running in application space, an offset (pointer) to enable location of the base address of the data within the kernel space (pg. 19).

As per claim 11, D22 teaches providing to the application a list of offsets with respect to the offset of the base address (pg. 19).

As per claim 12, D22 teaches the data is received as data frames from a network link (pg. 60).

As per claim 13, D22 teaches adding to substantially each of the received data frames a descriptor, the descriptor containing data relating to the data frame to which it is attached (pg. 19, capture length).

As per claim 14, D22 teaches a network analyzer card (pg. 55) for connection to a host and a network, the card comprising:  
a receiver for receiving plural data frames from a network link (pg. 7);  
data replication means for generating at least two replica editions of the received data frames (pgs. 18-19 and Fig. 2.6); and  
a descriptor adder configured and arranged to add a descriptor [header] to substantially each of the data frames of each of the at least two replica editions of the received data frames, the descriptor including data about the data frame [data length] to which it is attached for use in processing of the data frame (pg. 19).

As per claim 15, D22 teaches data writing means for writing the at least two replica editions of the received data frames to an area of host memory directly accessible by a host application (pg. 19, shared memory).

As per claim 16, D22 teaches the descriptor includes data indicative of the length of a data frame to which it is attached (pg. 19).

As per claim 17, D22 teaches the descriptor includes a timestamp indicative of the time at which the corresponding data frame was received at the network analyzer card (pg. 19).



As per claim 18, D22 teaches one or more of the data replication means, the descriptor adder and the data writing means is or are arranged in hardware (pg. 6).

As per claim 19, D22 teaches receiving data from a network link (pgs. 10 and 17);

replicating said data on board a network analyzer card (pg. 55) to produce at least two editions of the received data (pgs. 18-19 and Fig. 2.6); and

writing said editions of the received data to an area of memory in a host that is directly accessible by a host application (pg. 19 and 25, section 2.7.4).

As per claim 20, D22 teaches a host comprising:

a network analyzer card (pg. 55) for receiving data from the network

a memory to receive at least two editions of the received data from the network analyzer card (pg. 19, shared memory); and

at least two processors for processing said editions of the received data (pg. 7 and 27, plural processors including a dual processor);

a receiver for receiving plural data frames from a network link (pg. 7);  
data replication means for generating at least two replica editions of the received data frames (pgs. 18-19 and Fig. 2.6); and

a descriptor adder configured and arranged to add a descriptor [header] to substantially each of the data frames of each of the at least two replica editions of the received data frames, the descriptor including data about the data frame [data length] to which it is attached for use in processing of the data frame (pg. 19).

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 21-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over D22 in view of USP 4,837,735, to Allen et al., hereinafter Allen.

As per claim 21, D22 teaches running this network device with more than one processor. On page 7, D22 mentions networks processors and even runs the device using a dual core processor on page 27. D22 also teaches that the sets of rules are run independently in their own flow according to a particular rule (pg. 58). While D22 teaches the use of more than one processor and running rules independently, there is no explicit teaching of assigning a set of rules to each processors but this is an obvious step in view of Allen. Allen teaches that each processor is responsible for running through a unique rule set (col. 15, lines 50-55). It is also known that dual processors are in fact designed for parallel processing to achieve greater throughput. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to

Art Unit: 2431

combine the teachings of D22 and Allen to use each processor to check data against sets of rules to improve greater throughput of the system.

As per claim 22, D22 teaches the rules relate to intrusion detection (pg. 57).

As per claim 23, D22 teaches the processors are arranged to execute rules of an intrusion detection system on data packets received by the host (pg. 57).

### ***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is

Art Unit: 2431

(571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/Ayaz R. Sheikh/

Supervisory Patent Examiner, Art Unit 2431